Spam and Cybercrime

SMTP

- Simple Mail Transfer Protocol
  - Client connects to server on TCP port 25
  - Client sends commands to server
  - Server acks or notifies of error
- Security issues
  - Sender not authenticated
  - Message and headers transmitted in plain text
  - Message and header integrity not protected
  - Spoofing trivial to accomplish

- Example SMTP session

HELO mail.university.edu

MAIL FROM: president@whitehouse.gov

RCPT TO: chancellor@university.edu

DATA

From: president@whitehouse.gov

To: chancellor@university.edu

Date: April 1, 2010

Subject: Executive order

You are hereby ordered to increase the stipend of all TAs by $10,000 per year.

Sincerely,

The President of the United States

.

What is Email Spam?

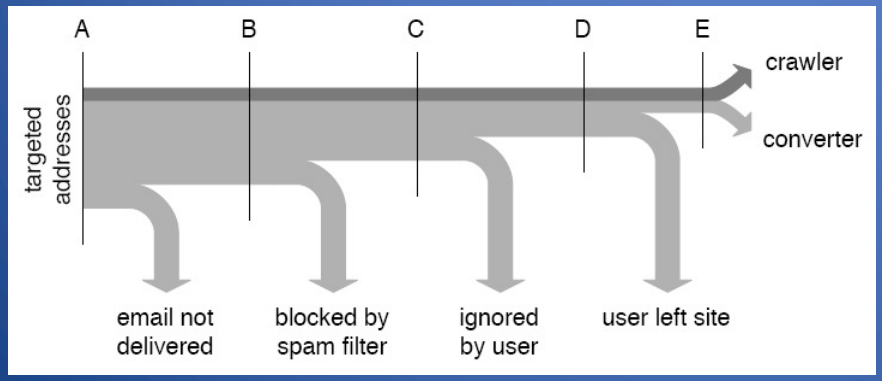
- Email spam is often defined as unsolicited bulk email
  - Forbidden by all major ISPs
  - Considered “acceptable business practice” by US Direct Marketing Association (DMA)
- Unsolicited email and bulk email are individually acceptable practices for people, business, and organizations
- Spam arises from the combination of unsolicited and bulk
- In classifying email as spam, content does not matter
- The US CAN-SPAM act (2004) regrettably protects commercial spam provided some requirements are satisfied, including:
  - Opt-out mechanism
  - Sender clearly identified and subject line not deceptive
  - Adult material labeled in subject line

Who Responds to Spam anyhow?

A princess in Nigeria
wants to send me money!

Spam Conversion

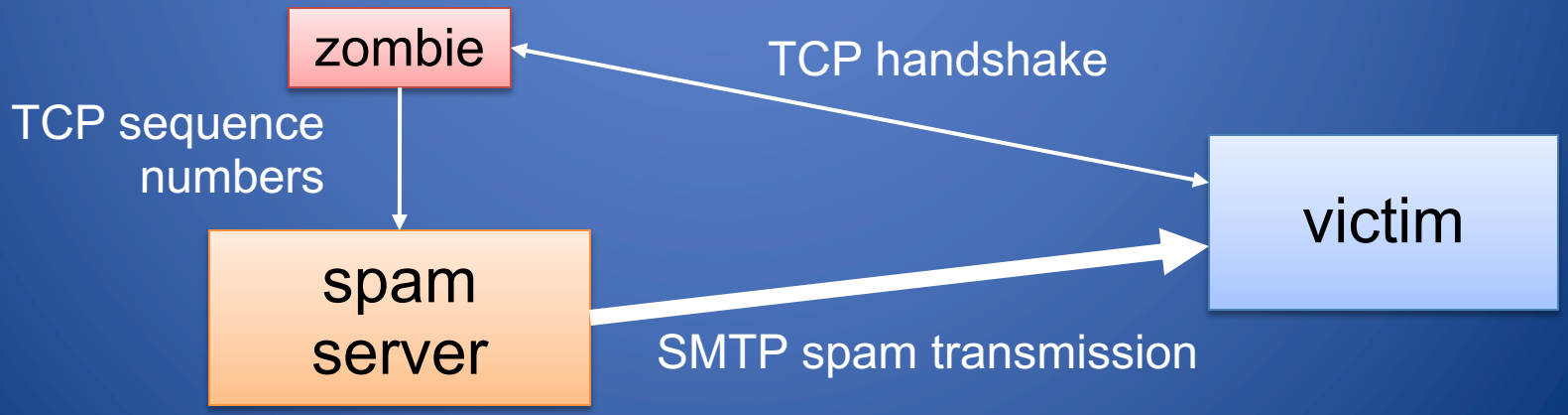
- Empirical study [Kanich+ 2008]
  - Parasitic infiltration into botnet launching spam campaign for "Canadian drugs"
  - 28 conversions, yielding $3K, from 300M spam messages over 26 days



Yes, Honey, you ***could*** benefit from that drug.

Blacklisting

- Spamhaus Black List (SBL)
  - Real-time database of IP addresses of verified spam sources
  - Eliminates about 10% of spam before transmission takes place
  - Formal listing and delisting procedures
  - More than 600M email users protected by SBL
- How to circumvent blacklisting
  - Powerful blacklisted spam server impersonates small unlisted zombie
  - Initiate TCP handshake from zombie
  - Send bulk email from spam server using spoofed source IP and TCP sequence numbers

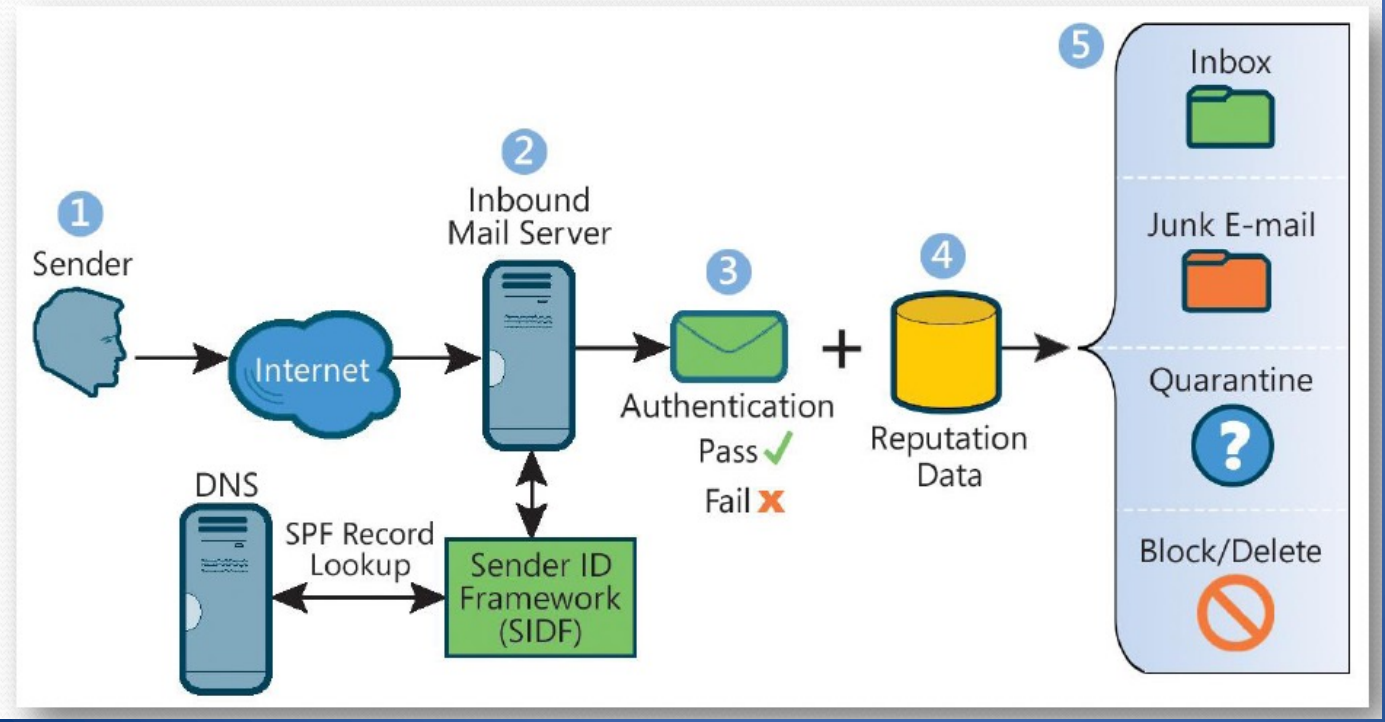


Graylisting

- Spam servers typically do not resend messages after transmission errors
- Maintain database of trusted servers
- Respond with “Busy, please retry” to SMPT connection requests from servers not in database
- Server added to database if reestablishes connection
- Currently effective although simple to circumvent

Sender ID and Sender Policy Framework

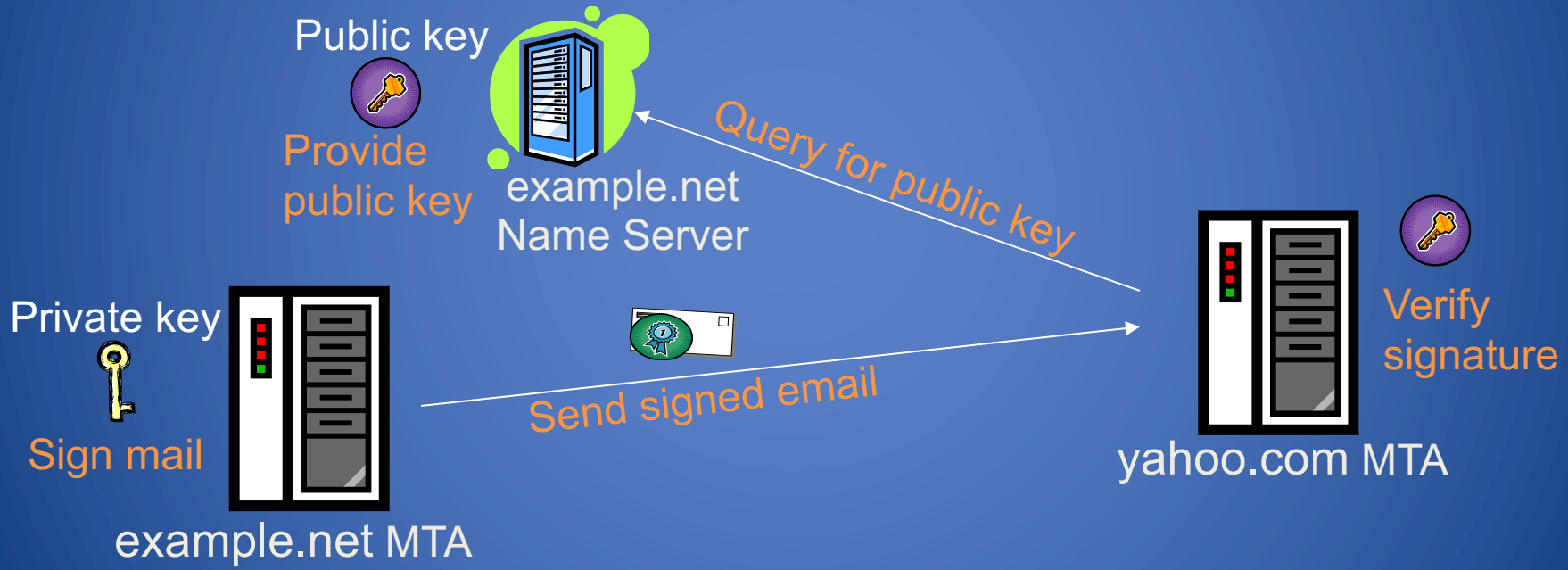
- Store DNS records about severs authorized to send mail for a given domain
- Look up domain in From header to find IP address of authorized mail server



Source: Microsoft

DomainKeys Identified Mail (DKIM)

- Sender's mail server signs email to authenticate domain
- Public key of server available in DNS record
- To be used in conjunction with other spam filtering methods



DomainKey-Signature: a=rsa-sha1; s=mail; d=example.net; c=simple; q=dns; b=Fg…5J

Authentication-Results: example.net from=bob@example.net; domainkeys=pass;

SenderID vs. DKIM

SenderID

- Sending MTA authentication
- Channel based
- Simple implementation
- Message integrity not protected
- Mail forwarding not supported
- Vulnerable to DNS cache poisoning
- Vulnerable to IP source spoofing

DKIM

- Sending MTA authentication
- Object based
- Cryptographic assurance
- Protection of message integrity
- Supports mail forwarding
- Vulnerable to DNS cache poisoning

Cybercrime

- Symantec's definition:
  - Cybercrime is any crime that is committed using a computer, network, or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. The crime may take place on the computer alone or in addition to other locations.
- Enablers of cybercrime
  - Software vulnerabilities
  - Online shopping and access to financial accounts
  - Countries with lax or corrupt law enforcement

Credit Cards

- Credit card information
  - Supposed to be kept secret
  - Shared with multiple merchants
  - Transmitted often insecurely
  - Low entropy of the credit card number (first four digits denote financial institution)
- Advantage
  - Simple scheme for users, banks, and merchants
- Disadvantage
  - Fraud easy to commit
- Tradeoff
  - No security measures to facilitate use
  - Private customers and merchants held harmless
  - Transaction fee covers bank fraud losses

Common Credit Card Frauds

- Buy popular goods and resell them
  - Needs package delivery address
  - Requires resale business
  - Often goods reshipped abroad
- Buy financial instruments
  - Traveler's checks
  - Gift cards
  - E-gold
  - Additional conversion needed to avoid revocation
- Buy cash equivalents
  - Western Union money transfers
  - Foreign currency

Defending Against Credit Card Fraud

- One-time credit card numbers
  - Available from several issuers (e.g., AmEx, Citibank)
  - Does not work for subscription plans
  - Time consuming for users
  - Cumbersome to obtain refunds
  - Worthwhile for high-value transactions or untrusted merchants
- Monitoring transactions
  - Email or text message for each transaction
  - Continuous annoyance to catch a rare event
- Password enabled transactions
  - Similar to PIN for ATM cards
  - Difficult to share password only with the bank and communicate verification outcome to merchant (three-party protocol)

Bank Accounts

- Account information
  - Supposed to be kept secret
  - Shared with merchants, customers and friends
  - Same account number for deposits and withdrawals
- Typical bank transactions
  - Check
  - ATM
  - Wire transfer
- Banking in the US
  - Account title
  - Taxpayer ID Number (TIN)
  - Checks can be generated by customers or third parties
  - Signature not verified in practice for amounts below $30K
  - Automated Clearing House (ACH), regulated by Federal Reserve, supports interbank transfers, direct deposits and direct debits
  - ACH allows one to initiate from account A an inbound transfer into A from any account B with same TIN as A

Common Bank Frauds

- Forged checks
  - Create checks with magnetic ink printers
  - Cash with fake ID
  - Low amounts typically not scrutinized
- Wire transfer
  - Send fax to bank to order wire transfer
  - Most effective if money wired abroad
- Account creation
  - Create account A impersonating owner of account B
  - ACH transfer from B to A
  - Cash with ATM or wire transfer

Defending Against Bank Fraud

- Multi-factor authentication
  - Hardware token generating one-time codes
  - Personal images and sentences to defend against phishing
  - Code sent by email/sms to registered address to authorize debit transactions
- Account ownership verification
  - Linking accounts for ACH transfers requires knowledge of to small deposits to the account
- Restrictions on accounts
  - E.g., only credit transaction accepted
- Monitoring bank transactions
  - Email/text message after each transactions
- No online banking
  - Limited bank liability for online frauds